UNITED STATES DISTRICT COURT
FO THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

ROSALYN PARKER, individually and on behalf of all others similarly situated, Plaintiff, v. THE DUFRESNE SPENCER GROUP, LLC d/b/a ASHLEY FURNITURE HOMESTORE, Defendant.	Civil Action No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Rosalyn Parker ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against The Dufresne Spencer Group, LLC d/b/a Ashley Furniture HomeStore ("Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against Defendant challenging its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII"), including names, dates of birth, driver's licenses, banking information (i.e., account number, routing number), digital signatures, among other personal information (collectively, the "Private Information") from cybercriminals.

2. On or about January 15, 2024, Defendant learned that an unauthorized party had gained access to its information technology environment between May 15, 2023 – June 5, 2023;

and during that time the unauthorized party accessed and/or acquired files on Defendant's systems which contain personal information (the "Data Breach"). Defendant reviewed the files compromised in the Data Breach, and determined that Plaintiff's and other similarly situated Class Members had their name, date of birth, driver's license, banking information (i.e., account number, routing number), and digital signature accessed and/or acquired by an unauthorized party in the Data Breach.

3. As a result of the Data Breach, and in light of their Private Information now being in the hands of cybercriminals, Plaintiff and Class Members were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. This substantial and imminent risk will remain for their respective lifetimes.

4. Armed with the Private Information accessed in the Data Breach, the cybercriminals who carried out the Data Breach can and will commit a variety of crimes, including, *e.g.*, obtaining medical services and/or prescriptions in Class Members' names, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

5. There has been no assurance offered by Defendant that all personal data or copies of data have been recovered or destroyed, or that it has adequately enhanced its data security practices sufficiently to avoid a similar breach of its network in the future.

6. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm

from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

7. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained in its systems.

8. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

9. Upon information and belief, Defendant failed to properly monitor and implement adequate data security practices with regard to its computer network and systems that housed Plaintiff's and Class Members' Private Information. Had Defendant properly monitored its networks and implemented adequate data security practices, it could have prevented the Data Breach or, at the very least, discovered the Data Breach sooner.

10. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct, which led to the Private Information that it collected and maintained falling into the hands of data thieves and other unauthorized third parties.

11. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and exfiltrated during the Data Breach.

//

//

//

PARTIES

12. Plaintiff is, and at all times mentioned herein was, an individual citizen and resident of the State of Texas.

13. Defendant is a large home furnishings retailer consisting of 166 Ashley HomeStore locations and 21 distribution centers across the United States (Arkansas, Tennessee, Kentucky, Texas, Indiana, Illinois, Michigan, Ohio, Mississippi, Louisiana, Missouri, and New Mexico) and Canada, over 5,000 team members, and is the largest Ashley licensee in the world. In 2021, Defendant had $1.2 billion in sales in the USA and has been the "#1 Furniture Retailer in the world for 15 consecutive years."[1] Defendant is a limited liability company formed in the State of Delaware with a corporate headquarters or principal place of business located at 4120 Air Trans Road, Memphis, Tennessee.

JURISDICTION AND VENUE

14. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of Class Members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

15. This Court has jurisdiction over Defendant because Defendant operates and does business within this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred within this District and Defendant has harmed Plaintiff and other Class Members residing in this District.

[1] https://ashleydsg.com/about/ (last accessed June 6, 2024)

FACTUAL ALLEGATIONS

Defendant's Business and Collection of Plaintiff's and Class Members' Private Information

17. Defendant is a large home furnishings retailer consisting of 166 Ashley HomeStore locations and 21 distribution centers across the United States and Canada, and is the largest Ashley licensee in the world. In 2021, Defendant had $1.2 billion in sales in the USA and has been the "#1 Furniture Retailer in the world for 15 consecutive years." As a condition of receiving goods and/or services from and/or being employed with Defendant, customers and employees are required to entrust Defendant with highly sensitive personal information and Private Information.

18. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its customers and employees, Defendant promises to, among other things, keep their Private Information private; comply with industry standards related to data security and the maintenance of their Private Information; inform its customers and employees of its legal duties relating to data security and comply with all federal and state laws protecting their Private Information; only use and release customers' and employees' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers and employees if their Private Information is disclosed without authorization.

19. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

20. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this data, which Defendant ultimately failed to do.

The Data Breach and Defendant's Inadequate Notice to Plaintiff and Class Members

21. According to Defendant's notice of the Data Breach, it learned of unauthorized access to its systems which occurred between May 15, 2023 – June 5, 2023 on or around January 15, 2024. Defendant did not begin disseminating notice of the Data Breach until several months later.

22. On or around May 7, 2024, Plaintiff and the Class Members began receiving notices of the Data Breach, informing them that its investigation determined that their Private Information was impacted, and an unauthorized party accessed and/or acquired their Private Information on Defendant's systems.

23. The notice letter then listed time-consuming, generic steps that victims of data security incidents can take, and encouraged Plaintiff and the Class Members to remain vigilant by reviewing [their] financial account statements and credit reports for any unauthorized activity. Other than providing only a one-year membership of credit monitoring and identity theft protection through Equifax Credit Watch Gold, Defendant offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves from the aftermath of the Data Breach. On information and belief, Defendant sent a similar generic letter to all other individuals affected by the Data Breach.

24. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from access, disclosure, and exfiltration by unauthorized parties.

25. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its

obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

26. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years. Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

Defendant Failed to Comply with FTC Guidelines

27. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

28. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

29. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

30. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

31. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

32. Defendant was at all times fully aware of its obligation to protect the Private Information of its customers and employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards and Best Practices

33. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

34. Some industry best practices that should be implemented by businesses dealing with sensitive PII like Defendant include but are not limited to: education of all employees, strong

password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

35. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

36. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

37. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur, resulting in harm to Plaintiff and the Class Members.

Defendant Breached its Duty to Safeguard Plaintiff's and Class Members' Data

38. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty

to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

39. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customer and employee Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of customer and employee Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA; and

f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

40. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

41. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in

the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

42. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

Defendant Should Have Known that Cybercriminals Target Private Information and PII

43. The FTC hosted a workshop to discuss "informational injuries," which are injuries that individuals like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[2] Exposure of highly sensitive personal information that an individual wishes to keep private may cause harm to that individual, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

44. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

45. Because a person's identity is akin to a puzzle, the more accurate pieces of data an

[2] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf

identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

46. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

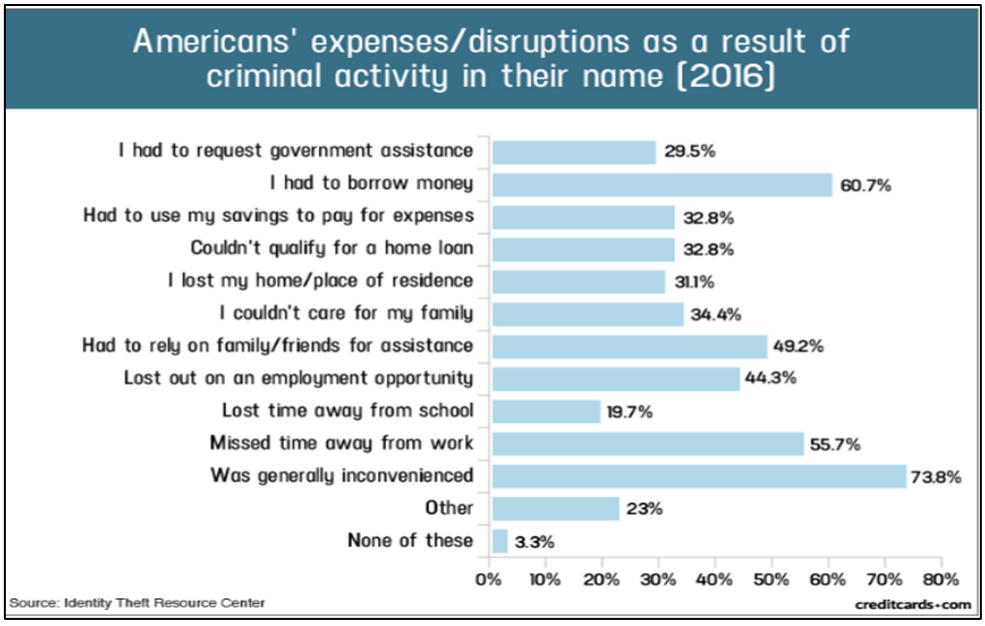
47. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

48. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.[3] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

49. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

50. In fact, a study by the Identity Theft Resource Center[4] shows the multitude of harms caused by fraudulent use of PII:



51. The ramifications of Defendant's failure to keep its customers' and employees' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such

[3] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps

[4] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on April 10, 2024).

and damage to victims may continue for years.

52. Here, not only were sensitive unique Defendant financial account numbers information compromised, but driver's licenses and digital signatures were compromised too. The value of personal information including PII is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

53. PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

54. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

Plaintiff's and Class Members' Damages

55. Plaintiff was a customer of Ashley Furniture HomeStores and financed furniture purchased through Defendant, and provided her Private Information to Defendant in order to receive Defendant's home furnishing goods and/or services.

56. On or about May 7, 2024, Plaintiff received notice from Defendant alerting her that her Private Information had been accessed and exfiltrated in the Data Breach.

57. The notice letter offered Plaintiff only one (1) year of credit monitoring services – an insufficient remedy considering Plaintiff has and will now continue to experience a lifetime of increased risk of identity theft.

58. Plaintiff suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her

accounts for fraud. Furthermore, Plaintiff suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach. Specifically, Plaintiff has suffered invasion of privacy, identity theft, fraudulent accounts opened using her Private Information and PII, multiple unauthorized credit inquiries, damage to her credit, and denial of credit applications, which she attributes to the Data Breach.

59. Plaintiff would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its her Private Information from unauthorized access and exfiltration, and that those systems were subject to a data breach.

60. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of being an employee for Defendant and which was compromised in, and as a result of, the Data Breach.

61. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

62. Plaintiff has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

63. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to reviewing financial accounts for any indications of actual or attempted identity theft or fraud, monitoring and freezing her credit reports. Plaintiff has already spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

64. As a result of the Data Breach, Plaintiff has suffered stress and anxiousness as a result of the invasion of her privacy and unauthorized release of her Private Information, which she believed would be protected from unauthorized access and exfiltration. These feelings include distress about unauthorized parties having, viewing, selling, and/or using her Private Information, including PII, for purposes of committing cyber crimes and other crimes against her or others, including, but not limited to, fraud and identity theft. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will continue to have on her life.

65. Plaintiff also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

66. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to remain vigilant to mitigate and address the many harms caused by the Data Breach.

67. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

68. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's goods and/or services.

69. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

70. As a direct and proximate result of Defendant's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

71. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

72. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

73. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

74. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent activities against Plaintiff and Class Members.

75. Plaintiff and Class Members also lost the benefit of the bargain they made with

Defendant. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price paid by Plaintiff and Class Members (or, in some cases, on their behalf) to Defendant for its goods and/or services was intended to be used by Defendant to fund adequate security of Defendant's system and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive the benefit of the bargain.

76. Additionally, Plaintiff and Class Members also suffered a loss of value of their Private Information and PII when it was accessed and/or acquired by cyber criminals as a result of the Data Breach.

77. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[5] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[6]

78. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with

[5] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion.

[6] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

79. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

80. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendant, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal information of its customers and employees is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

81. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

CLASS ACTION ALLEGATIONS

82. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

83. Specifically, Plaintiff proposes the following Class, subject to amendment as appropriate:

> **All individuals whose Private Information was compromised in the May 15, 2023 – June 5, 2023 Data Breach, for whom notice letters were sent on by or on behalf of Defendant.**

84. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

85. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

86. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

87. Numerosity – The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of hundreds of thousands of individuals whose Private Information was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

88. Commonality – There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant's response to the Data Breach was adequate;

e. Whether Defendant unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

j. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

p. Whether Defendant's conduct was negligent;

q. Whether Defendant was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

89. Typicality – Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff individually. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

90. Adequacy of Representation – Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

91. Superiority – A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

92. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data

Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
NEGLIGENCE

93. Plaintiff restates and realleges all of the allegations in every preceding paragraph as if fully set forth herein.

94. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

95. Defendant knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Defendant was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

96. Defendant owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Defendant's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

e. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

97. Defendant's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

98. Defendant's duty also arose because Defendant was bound by industry standards to protect Plaintiff and the Class Members' Private Information.

99. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Defendant owed them a duty of care to not subject them to an unreasonable risk of harm.

100. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

101. Defendant, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

102. Defendant, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

103. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA; and

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

104. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems (and the Private Information that it stored on them) from attack.

105. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, accessed, exfiltrated, and/or misused, as alleged herein.

106. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

107. Defendant's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

108. As a result of Defendant's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

109. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

110. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

111. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

112. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

113. Plaintiff restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

114. Defendant is a furnishings retailer that provided goods and/or services and/or employment to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those goods and/or services through their collective conduct, including by Plaintiff and Class Members turning over their valuable Private

Information to Defendant.

115. Through Defendant's offering of these goods and/or services and/or employment, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with Defendant's policies, practices, and applicable law.

116. As consideration, Plaintiff and Class Members turned over valuable Private Information to Defendant. Accordingly, Plaintiff and Class Members bargained with Defendant to securely maintain and store their Private Information.

117. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of receiving goods and/or services and/or employment to Plaintiff and Class Members.

118. In delivering their Private Information to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the Private Information as part of that service.

119. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (8) taking other steps to protect against foreseeable data breaches.

120. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

121. Had Defendant disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Defendant and would have sought home furnishing goods and/or services and/or employment elsewhere.

122. Defendant knew or should have known that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the other Class Members.

123. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete Private Information to Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Private Information.

124. Plaintiff and Class Members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT

125. Plaintiff restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

126. This cause of action is pleaded in the alternative to Plaintiff's second cause of action above.

127. Plaintiff and Class Members conferred a benefit on Defendant by turning over their valuable Private Information to Defendant with the understanding that the benefits earned from possession and control thereof would be utilized, in part, to provide adequate data security to protect such Private Information. Plaintiff and Class Members did not receive such protection.

128. Defendant knew that Plaintiff and Class Members conferred a benefit upon it

and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

129. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

130. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

131. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information with Defendant or become employees and/or customers of Defendant.

132. Plaintiff and Class Members have no adequate remedy at law.

133. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

134. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) dissemination of their Private Information on the dark web; (ix) statutory damages; (x) nominal damages; and (xi)

the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

135. It would be inequitable for Defendant to retain the benefit of controlling and maintaining Plaintiff's and Class Members' Private Information at the expense of Plaintiff and Class Members.

136. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

137. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT & INJUNCTIVE RELIEF

138. Plaintiff restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

139. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state

statutes described above.

140. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

141. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continue to owe a legal duty to secure the sensitive personal information with which they are entrusted, specifically including information obtained from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Defendant breached, and continue to breach, their legal duty by failing to employ reasonable measures to secure their customers' personal information; and,

c. Defendant's breach of their legal duty continues to cause harm to Plaintiff and the Class.

142. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its users' data.

143. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an

adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

144. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

145. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action, certifying the Class as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper and adequate Class Representative;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, punitive damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying Class Members

about the judgment and administering the claims process;

e. An order requiring Defendant to implement enhanced data security practices in order to better protect the Private Information and PII in its possession and control;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowed by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff is entitled to, and demands, a trial by jury on all issues so triable.

Dated: June 10, 2024

Respectfully submitted,

By: */s/ Abbas Kazerounian*

Abbas Kazerounian (TX SBN: 24090982)
Mona Amini, Esq. (*pro hac vice forthcoming*)
KAZEROUNI LAW GROUP, APC
245 Fischer Ave., Unit D1
Costa Mesa, CA 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff